REMARKS

Claims 1-5, 7, 10-14, and 16 are pending in the present application.

Claims 1-5, 7, 10-14, and 16 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Carson (U.S. Patent Number 6,477,124) in view of Atkinson (U.S. Patent Number 6,694,451). Reconsideration of the rejections and allowance of claims 1-5, 7, 10-14 and 16 are respectfully requested.

In the present invention as claimed in independent claim 1, a method of authenticating a digital medium by determining the presence of an anomaly region corresponding to a data segment of the digital medium includes performing multiple read operations on a data segment of the medium to generate multiple corresponding read data results, calculating corresponding digital signatures using actual data values of underlying data of the read data segment for each of the multiple read data results, and determining whether an anomaly region is present in the data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value. If a predetermined number of the digital signatures are not equal in value, the anomaly region is determined to be present. Further, the method includes authenticating the medium in response to the determination of the presence of the anomaly region.

In the present invention as claimed in independent claim 10, a system for authenticating a digital medium by determining the presence of an anomaly region corresponding to a data segment of the digital medium that includes a read unit for performing multiple read operations on a data segment of the medium to generate multiple corresponding read data results, a calculating unit for calculating corresponding digital signatures using actual data values of the read data segment for each of the multiple read data results, and a determining unit for determining whether an anomaly region is present in the data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value. If a predetermined

number of the digital signatures are not equal in value, the determining unit determines the anomaly region to be present. Further, the system includes a means for authenticating the medium in response to the determination of the presence of the anomaly region

As stated in Amendment A dated February 15, 2008 and the Amendment dated November 10, 2008, Carson discloses, at column 5, lines 7-25, that data on an optical disk can be read from beginning to end or from "lead-in" to "lead-out," or can be accessed in a non-contiguous fashion. Carson further discloses, at column 8, lines 7-43 and at column 9, lines 14-67, a process for disk authentication based on a data rate at which data are written to and read from a disk. In Carson, a data rate profile indicative of the data rate at which data are written to the disk is stored on a disk and used for disk authentication. The data are intentionally written at different, or varying, speeds, at different locations on the disk, and a measured data rate as a function of position on the disk is used to create the data rate profile. Variance in the data rate at which data are written to the disk results in the pits and lands written to the disk having different sizes, depending on the velocity of the disk at the time and position at which the given pits and lands are written. Authentic disks will include data that are recorded in accordance with the data rate profile and non-authentic disks will not. During playback, a readback system will attempt to speed up and slow down the rotation of the disk to maintain a substantially constant recovered data rate. The behavior of the readback system during readback is monitored, recorded, and analyzed to form a data rate profile for the disk in question. When an unauthorized duplicate disk is created, the expected data rate profile will not be present on the unauthorized duplicate disk because an unauthorized disk will not have variance in the lengths of its pits and lands at expected locations on the disk. During a subsequent reading operation of a disk, the actual velocity of the disk at certain locations can be compared to the expected velocity at those locations to authenticate the disk. If a mismatch occurs, the disk is determined to be an unauthorized disk and access to the disk can be prevented. If no mismatch is detected, full disk access can be granted.

Further, as stated in Amendment A dated February 15, 2008 and the Amendment dated November 10, 2008, in the invention as claimed in claims 1 and 10, an anomaly

region is determined to be present on the disk in the event that a predetermined number of the digital signatures resulting from the underlying data read during the multiple read operations are "not equal in value," or different. In contrast, Carson teaches the inverse; namely that an anomaly region (different sized pits and lands) is determined to be present on the disk in the event that the data rate profiles (measured and expected) are determined to be equal in value, or the same.

Therefore, Carson fails to teach or suggest a method of determining the presence of an anomaly region in a digital medium which includes "determining whether an anomaly region is present in" a "data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, determining the anomaly region to be present," as claimed in independent claim 1. In addition, Carson fails to teach or suggest a system for authenticating a digital medium by determining the presence of an anomaly region corresponding to a data segment of the digital medium which includes "a determining unit for determining whether an anomaly region is present in" a "data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, the determining unit determining the anomaly region to be present," as claimed in independent claim 10.

Atkinson discloses that a CPU detects initiation of a low power state and reads each page of memory. For each page of memory the CPU calculates a signature for that page. After the signature is calculated, that page of memory is saved to the hard drive and the signature is saved to either non-volatile memory or to volatile memory. When the system resumes from suspend mode, the CPU reads a page of system memory and calculates the signature. The calculated signature is then compared with the saved signature value. If the signatures match, the data for that page is assumed valid. If the signatures do not match, the data in that page is assumed to be invalid.

Like Carson, Atkinson fails to teach or suggest a method of determining the presence of an anomaly region in a digital medium which includes "determining whether an anomaly region is present in" a "data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, determining the anomaly region to be present," as claimed in independent claim 1. Like Carson, Atkinson further fails to teach or suggest a system for authenticating a digital medium by determining the presence of an anomaly region corresponding to a data segment of the digital medium that includes "a calculating unit for calculating corresponding digital signatures using actual data values of underlying data of the read data segment for each of...multiple read data results," and "a determining unit for determining whether an anomaly region is present in" a "data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, the determining unit determining the anomaly region to be present," as claimed in independent claim 10.

As noted above, in the invention as claimed in claims 1 and 10, an anomaly region is determined to be present on the disk in the event that a predetermined number of the digital signatures resulting from the underlying data read during the multiple read operations are "not equal in value," or different. Instead, in Atkinson if the saved signature and the calculated signature match, then the page is assumed to be valid.

Carson and Atkinson fail to teach or suggest elements of the invention set forth in independent claims 1 and 10-14. Specifically, neither of the references teaches or suggests a method of determining the presence of an anomaly region in a digital medium which includes "determining whether an anomaly region is present in" a "data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, determining the anomaly region to be present," as claimed in independent claim 1, or a system for authenticating a digital medium by determining the presence of an anomaly region corresponding to a data segment of the digital medium

that includes "a calculating unit for calculating corresponding digital signatures using actual data values of underlying data of the read data segment for each of...multiple read data results," and "a determining unit for determining whether an anomaly region is present in" a "data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, the determining unit determining the anomaly region to be present," as claimed in independent claim 10. Accordingly, there is no combination of the references which would provide such teaching or suggestion.

Neither of the references, taken alone or in combination, teaches or suggests the invention set forth in independent claims 1 and 10. Furthermore, the differences between the combination of Carson and Atkinson and the claimed invention would not be obvious to one of ordinary skill in the art. Therefore, it is believed that the claims are allowable over the cited references, and reconsideration of the rejection of independent claim 1 and 10 under 35 U.S.C. 103(a) as being unpatentable over Carson and Atkinson, is respectfully requested. With regard to the dependent claims 2-5, 7, 11-14, and 16, it follows that this claim should inherit the allowability of the independent claims from which they depend.

Closing Remarks

It is submitted that all claims are in condition for allowance, and such allowance is respectfully requested. If prosecution of the application can be expedited by a telephone conference, the Examiner is invited to call the undersigned at the number given below.

In connection with this matter, please charge any otherwise unpaid fees which may be due or credit any overpayment to Deposit Account Number 50-1798.

Respectfully submitted,

Date: July 21, 2009

Mills & Onello, LLP
Eleven Beacon Street, Suite 605
Boston, MA 02108
Telephone: (617) 994-4900, Ext. 4902
Facsimile: (617) 742-7774
J:\ECD\0014CIP\OA_12209\Response_012209OA.doc

Anthony P. Onello, Jr.
Registration Number 38,572
Attorney for Applicant